The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
https://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/04/2020

SUBJECT:
A Vulnerability in GNU C Library Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in the GNU C Library (glibc), which could allow for remote code execution. This library is required in all modern distributions of Linux as it defines the system calls and other basic facilities used in the Linux kernel. Successful exploitation of this vulnerability could allow an attacker to execute remote code in the context of the affected application. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in a denial-of-service condition.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- GNU C Library versions 2.32 and prior

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:
A vulnerability has been discovered in the GNU C Library (glibc), which could allow for remote code execution. Specifically, this is a stack-based-buffer-overflow due to the __ieee754_rem_pio2l() function's failure to validate pseudo-zero values. This vulnerability can be exploited when the system processes maliciously crafted data.

Successful exploitation of this vulnerability could allow an attacker to execute remote code in the context of the affected application. Depending on the privileges associated with the

application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in a denial-of-service condition.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patched provided by the affected *nix distribution to the vulnerable systems after appropriate testing.
- Verify no unauthorized system modifications have occurred on the system before applying the patch.
- Run all software as non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Red Hat:
https://access.redhat.com/security/cve/cve-2020-10029

Debian:
https://security-tracker.debian.org/tracker/CVE-2020-10029

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10029